METHOD AND SYSTEM FOR MANAGING TOKEN IMAGE REPLACEMENT

CROSS-REFERENCES TO RELATED APPLICATION

[0001] The present application claims the benefit of priority under 35 U.S.C. § 119 from U.S. Provisional Patent Application Serial No. 60/410,555, entitled "METHOD AND SYSTEM FOR MANAGING CARD IMAGE REPLACEMENT", filed on September 13, 2002, the disclosure of which is hereby incorporated by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

[0002] The present invention generally relates to card image replacement and, more specifically, to a method and system for managing card image replacement on a smartcard via a computer network.

[0003] The emergence of secured tokens, such as smartcards, has allowed a much higher volume of information to be stored on a transaction card. For instance, in addition to the typical cardholder information, a smartcard is able to store a variety of different programs including, for example, a loyalty program of which the cardholder is a participant. Furthermore, unlike cards with magnetic stripes which can only retain static information, the use of a smartcard allows information stored thereon to be changed dynamically. As a result, there is often a need to update or replace contents of a smartcard.

[0004] Moreover, smartcards often need to be replaced for any number of reasons. Due to the transit time needed for replacement cards to reach their respective cardholders, these cards (such as a chip card that has the capability to receive updated information) generally do not contain the latest transaction information. This is because transactions conducted with the old card often occur during the transit period, i.e., the period between the issuance of the replacement card and the actual receipt of that card by its owner.

[0005] There are many different situations in which replacement cards are needed. One common situation is when an old card is about to expire. Typically when issuers, such as banks, replace a card, they do so by sending a replacement card to the cardholder in advance of the expiration date. Once the replacement card has been personalized and sent for delivery to the cardholder, there is a period of time that the cardholder may be conducting transactions on his/her existing card. In the case of a chip card, a cardholder may make

transactions that result in information being stored on the chip during the time the replacement card is in transit. As a result, when the replacement card is delivered to the cardholder, the most recent transaction information would not be captured on the replacement card.

[0006] Another common situation in which a replacement card is desired is when a card has been lost or stolen. Similar to the situation described above, the replacement card would not contain the most recent transaction information. Furthermore, in the case of lost or stolen cards, unauthorized and/or illegal transactions may have occurred. Therefore, it would be important to include the correct authorized transaction information on the replacement card.

[0007] Hence, it would be desirable to provide a method and system that is capable of facilitating card image replacement so as to allow replacement cards to be updated with the latest accurate transaction information in an intelligent and efficient manner.

BRIEF SUMMARY OF THE INVENTION

[0008] A system for managing token image replacement is provided. In an exemplary embodiment, the system includes a remote server, a personal computer (PC) connected to the remote server, a smartcard that can be read by the PC, and a card image server. Using application logic and rules, the remote server is able to read the card image on the smartcard and determine if the card image on the smartcard needs to be updated. If an indicator on the smartcard is set to "update", the remote server then retrieves a backup card image that corresponds to the card from the card image server. The remote server forwards the backup card image to the PC which, in turn, writes the backup card image including transaction information to the smartcard. Once the backup card image is written onto the smartcard, the indicator in the smartcard is then reset to ensure that subsequent interactions with the system would not initiate an update.

[0009] Reference to the remaining portions of the specification, including the drawings and claims, will realize other features and advantages of the present invention. Further features and advantages of the present invention, as well as the structure and operation of various embodiments of the present invention, are described in detail below with respect to accompanying drawings, like reference numbers indicate identical or functionally similar elements.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Fig. 1 is a simplified block diagram illustrating an exemplary embodiment of the present invention; and

[0011] Fig. 2 is a flow diagram further illustrating an exemplary method for managing token image replacement in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0012] The present invention in the form of one or more exemplary embodiments will now be described. Fig. 1 is a simplified block diagram illustrating an exemplary embodiment of the present invention. Referring to Fig. 1, according to one exemplary embodiment, the system 10 includes a remote server 12, a loyalty and account host 16, a token acceptance device 14 and a token 18. In other alternative exemplary embodiments (not shown), multiple instances of each component of the system 10 may be included. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know of other ways and/or methods to construct various system configurations in accordance with the present invention.

[0013] The loyalty and account host 16 maintains information on a number of loyalty programs and respective accounts relating to the loyalty programs. For example, the loyalty and account host 16 maintains backup token images of tokens 18 participating in the loyalty programs. A token image includes information relating to the holder of the token 18 or the loyalty program participant such as, loyalty programs that the holder is eligible to participate in and the associated account information, loyalty transactions completed, rewards earned and reward redeemed, etc. Optionally, the loyalty and account host 16 may maintain two or more backup token images for each token 18, depending on the particular design and/or constraints. The backup token images need not be identical. Various dated versions of the backup token images can be maintained. For example, a first backup token image for the token 18 may reflect information as of a first date, and a second backup token image for the same token may reflect information as of a second date. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods that can be used to maintain backup token images in accordance with the present invention. The loyalty and account host 16 can be implemented as a server or a computer that is capable of maintaining data or other information including token images, etc.

[0014] In one exemplary implementation, the token 18 is a smartcard. It should be understood that the token 18 includes other types of portable devices including, for example, a cellular phone, a personal digital assistant, a pager, a payment card (such as a credit card and an ATM card), a security card, an access card, smart media, a transponder and the like.

[0015] The token acceptance device 14 is a device that is capable of communicating with the token 18 including, for example, a point-of-sale device, a cellular phone, a personal digital assistant (PDA), a personal computer (PC), a tablet PC, a handheld specialized reader, a set-top box, an electronic cash register, a virtual cash register, a kiosk, a security system, an access system, and the like. In one exemplary embodiment, the token acceptance device 14 further includes a loyalty plug-in 22 and a loyalty transaction interface 24. As will be further described below, the loyalty plug-in 22 and the loyalty transaction interface 24 cooperate with one another as well as the remote server 12 to facilitate token image replacement.

[0016] The remote server 12 functions in cooperation with the loyalty and account host 16 and the token acceptance device 14 to facilitate maintenance of the token 18, as will be further described below. The remote server 12 is connected to the token acceptance device 14 and the loyalty and account host 16 via respective communication links, such as, a dialup connection, a leased line, a computer network including the Internet, and the like. The remote server 12 further includes an open program engine (OPE) 20. The OPE 20 contains application logic and rules that are used to manage and process loyalty transactions in connection with loyalty programs that are associated with the token 18. In addition, the application logic and rules in the OPE 20 are also used to facilitate maintenance of the token 18.

[0017] The system 10 operates in the following exemplary manner to complete token image replacement on the token 18. First, the token 18 is inserted into the token acceptance device 14 so that information on the token 18 can be retrieved. For example, using the application logic and rules, the remote server 12 is able to read the token image on the token 18 and determine if the token image on the token 18 needs to be updated. If an indicator on the token 18 is set to "update", the remote server 12 then retrieves a backup token image that corresponds to the token 18 from the loyalty and account host 16.

[0018] The indicator on the token 18 may be set to "update" in a number of ways. For example, in one situation, the indicator may be set by the issuer of the token 18 when the issuer forwards the token 18 to the holder. At the time the holder receives the token 18, the token 18 may be blank or contain minimal information. Hence, when the holder uses the token 18 to conduct loyalty program activities, the latest token image can be uploaded to the

token 18 to keep the token 18 current. In another situation, occurrence of a certain event might trigger the setting of the indicator to "update" so that additional information pertaining to the triggering event can be uploaded to the token 18.

[0019] As mentioned above, optionally, there may be two or more backup token images that can be uploaded to the token 18. Logic may be included to allow the appropriate backup token image to be uploaded. Various criteria can be used to determine which backup token image is to be uploaded. For example, a backup token image from a specific date may need to be uploaded to the token 18.

[0020] Once the backup token image is retrieved from the loyalty and account host 16, the backup token image is forwarded by the remote server 13 to the token acceptance device 14. The token acceptance device 14 then updates or writes the backup token image to the token 18. Typically, the entire backup token image is uploaded to the token 18. However, it should be noted that in some situations the token acceptance device 14 may choose to update the token 18 with selected portions of the backup token image. In other words, all or portions of the backup token image can be uploaded onto the token 18. This may be necessary to ensure that certain information that may have been added to the token 18 during prior transactions is not overwritten.

[0021] Once the backup token image is written onto the token 18, the indicator in the token 18 is then reset to ensure that subsequent interactions with the system 10 will not initiate an update.

[0022] Fig. 2 is a flow diagram further illustrating an exemplary method for managing token image replacement in accordance with the present invention. At 30, the loyalty plug-in 22 detects that an "update" is needed for the token 18. At 32, the loyalty plug-in 22 communicates with the loyalty transaction interface 24 which, in turn, issues an update request to the OPE 20. The update request includes information that is needed to identify the token 18. At 34, upon receiving the update request, the OPE 20 contacts the loyalty and account host 16 to retrieve the appropriate backup token image. The appropriate backup token image is determined based on information included in the update request. At 36, upon receiving the backup token image, the OPE 20 engages in mutual authentication with the token 18 with the help of the loyalty transaction interface 24. At 38, upon successful mutual authentication, the backup token image is passed by the OPE 20 to the loyalty plug-in 22 via the loyalty transaction interface 24. The loyalty plug-in 22 then updates the token 18 with the backup token image. At 40, the loyalty plug-in 22 then confirms the loyalty transaction interface 24 of the successful update. The loyalty transaction interface 24, in turn, forwards

the confirmation to the OPE 20. The OPE 20 stores the confirmation for subsequent reporting to the loyalty and account host 16.

[0023] The backup token image can also be provided to the token 18 in other exemplary manners. For example, the cardholder may contact a customer service representative to request an update (i.e., the backup token image) for the token 18. The customer service representative then, in turn, forwards an email to the cardholder with the backup token image attached. The backup token image can then be provided to the token 18. In another instance, the cardholder may contact the remote server 12 to request an update for the token 18. The remote server 12 may send the backup token image to a specific location, such as, a store. The store may have, for example, kiosks that allow the backup token image to be retrieved. The cardholder may then be instructed to visit the specific location to retrieve the backup token image. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know of other ways and/or methods to provide the backup token image to a token in accordance with the present invention.

[0024] In an exemplary embodiment, the system 10 as described above is implemented using a number of hardware and/or software components. It should be understood that in addition to the configurations described above, these components may be distributed in other manners, integrated or modular or otherwise, amongst the various components of the system 10 to achieve the same collective functionality, depending on factors such as the system design and resource constraints. For example, the open program engine 20 and the loyalty and account host 16 can be combined into a single remote server; and the loyalty plug-in 22 and the loyalty transaction interface 24 can be combined into single loyalty client. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know of other ways and/or methods to implement the functionality provided by the present invention in various forms and/or configurations.

[0025] The system 10 of the present invention as described above can be deployed in a number of applications. In one exemplary application, the system 10 can be used to update a newly issued smartcard with the most recent transaction information. After the newly issued smartcard is sent but before it is received by the cardholder, the cardholder may conduct transactions using his old smartcard during this interim period. Information relating to these transactions is captured on the backup smartcard image which is maintained by the loyalty and account host 16. This information, however, could not have been and is not stored on the newly issued smartcard. In addition, to improve security reasons associated with potential loss during transit, the new smartcard can be rendered blank or contain

minimal information when it is sent to the cardholder. Subsequently, when the cardholder receives the new smartcard, the system 10 allows the new smartcard to be updated with the backup smartcard image which includes the most recent transaction information captured during the interim period.

[0026] In another exemplary application, the system 10 can be used to update a newly issued smartcard with selected transaction information. This application is similar to the one described above except that selected transaction information is desired as opposed to the most recent. This may be desired in a situation where the new smartcard is issued to replace an old smartcard that has been stolen or lost. In this situation, the most recent transaction information may reflect fraudulent transactions. Hence, the new smartcard may need to be updated with information that existed at a certain point in time which is not necessarily the most recent. By using the system 10, the cardholder can update the new smartcard with the appropriate backup smartcard image to reflect only legitimate transactions that have been incurred. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods to deploy the present invention.

[0027] It is understood that the examples and embodiments described herein are for illustrative purposes only and that various modifications or changes in light thereof will be suggested to persons skilled in the art and are to be included within the spirit and purview of this application and scope of the appended claims. All publications, patents, and patent applications cited herein are hereby incorporated by reference for all purposes in their entirety.